BILLY J. WILLIAMS, OSB #901366
United States Attorney
District of Oregon
ETHAN D. KNIGHT, OSB #992984
GEOFFREY A. BARROW
CRAIG J. GABRIEL, OSB #012571
Assistant United States Attorneys
ethan.knight@usdoj.gov
geoffrey.barrow@usdoj.gov
craig.gabriel@usdoj.gov
1000 SW Third Ave., Suite 600
Portland, OR 97204-2902
Telephone: (503) 727-1000
Attorneys for United States of America

UNITED STATES DISTRICT COURT

DISTRICT OF OREGON

UNITED STATES OF AMERICA	**3:16-CR-00051-BR**
v.	**GOVERNMENT'S RESPONSE TO DEFENDANTS' MOTION TO SUPPRESS EVIDENCE (FACEBOOK ACCOUNTS) (#741)**
AMMON BUNDY, et al.,	
Defendants.	

The United States of America, by Billy J. Williams, United States Attorney for the District of Oregon, and through Ethan D. Knight, Geoffrey A. Barrow, and Craig J. Gabriel, Assistant United States Attorneys, hereby responds to defendants' Motion to Suppress Evidence (Facebook Accounts) (ECF No. 741) and the supporting Memorandum (ECF No. 742) filed by defendant Fry on behalf of all similarly situated defendants.

I. Government's Position

Because the warrant issued by U.S. Magistrate Judge Paul Papak satisfied the Fourth Amendment's particularity requirement and was supported by probable cause, the government

respectfully recommends that the Court deny defendants' Motion to Suppress Evidence from the Oregon Facebook warrant.

II. Procedural Background

On April 8, 2016, U.S. Magistrate Judge Paul Papak issued a search and seizure warrant for 23 Facebook accounts belonging to several defendants in this case. The warrant sought information associated with the 23 Facebook accounts operated by various defendants. Law enforcement timely executed the warrant on April 11, 2016, and Facebook subsequently provided materials to the government. According to the warrant's search protocols, law enforcement then segregated responsive materials from non-responsive materials as set forth in the warrant.

III. Legal Argument

In their Motion, "[d]efendants contend that the warrant was overbroad by authorizing the search and seizure of private email messages and other applications for which there was no probable cause." Defs.' Mem. 3. Defendants are mistaken.

A. The Warrant Is Not Overbroad

The Ninth Circuit considers three factors in analyzing the breadth of a warrant:

> (1) whether probable cause existed to seize all items of a category described in the warrant; (2) whether the warrant set forth objective standards by which executing officers could differentiate items subject to seizure from those which were not; and (3) whether the government could have described the items more particularly in light of the information available.

United States v. Flores, 802 F.3d 1028, 1044 (9th Cir. 2015) (quoting *United States v. Lei Shi*, 525 F.3d 709, 731-32 (9th Cir. 2008)).

In upholding a Facebook warrant in *Flores*, the Ninth Circuit found:

> The first two factors clearly suggest that the warrant was not overbroad. The warrant allowed the government to search only the Facebook account associated with [defendant's] name and email address, and authorized the government to seize only evidence of violations of [specific enumerated crimes]. The warrant also established "Procedures For Electronically Stored Information," providing executing officers with sufficient "objective standards" for segregating responsive material from the rest of [defendant's] account. *See Lei Shi*, 525 F.3d at 731-32.

Id.

Similarly, in the present case, the Facebook warrant at issue allowed the government to search only the 23 Facebook accounts listed in Attachment A to the warrant, identified by Uniform Resource Locators and associated with defendants' names. *See* Defs. ' Sealed Ex. B to ECF No. 742, at 3. Attachment B to the warrant authorized the government to seize only "evidence of violations of 18 U.S.C. § 372, Conspiracy to Impede a Federal Officer by Threat, Violence, or Intimidation." *See* Sealed Ex. B, at 6. Attachment B also outlines four paragraphs of detailed search procedures to guide law enforcement officers in executing the warrant, including instructions on segregating responsive materials from non-responsive materials. *See* Sealed Ex. B, at 7-8. Finally, the warrant here was even more particular than the lawful warrant in *Flores*, because unlike *Flores*, the present warrant contains a very narrow, three-month temporal limit: from the time period beginning on November 1, 2015, and ending on the date of the account holder's arrest (ranging from January 26, 2016, to February 11, 2016). *See* Sealed Ex. B, at 6.

Accordingly, the warrant here was particular in nature and not overbroad.

/ / /

B. The Warrant's Two-Step Process Is Specifically Authorized by Rule 41

Defendants' primary objection to the warrant seems to be that the above-mentioned particularity included in Sections II and III of Attachment B (i.e., criminal statute, search protocols for responsive materials, and time limitations) "do not narrow the scope of the overbroad warrant" because "[o]nce Facebook complied with the search warrant by disclosing the entirety of defendants' accounts, the government thereby 'seized' those accounts in their entirety." Defs.' Mem. 13. Defendants' argument is without merit.

Facebook's production (as described in Section I of Attachment B to the warrant) and law enforcement's subsequent search (as described in Sections II and III of Attachment B) were consistent with Rule 41's two-step procedure for warrants for electronic evidence. The government's use of this two-step process under Fed. R. Crim. P. 41 was reasonable under the Fourth Amendment.

1. Federal Rule of Criminal Procedure 41(e)(2)(B)

Rule 41(e)(2)(B) provides that a warrant "may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant. The time for executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review." The Advisory Committee Notes recognize that "electronic storage media commonly contain such large amounts of information that it is often impractical for law enforcement to review all of the information during execution of the warrant at the search location." Fed. R.

Crim. P. 41, comm. n. (e)(2) (2009 amend.). The Notes also state that "[t]his rule acknowledges the need for a two-step process: officers may seize or copy the entire storage medium and review it later to determine what electronically stored information falls within the scope of the warrant." *Id.* As authorized by Rule 41(e)(2)(B), the warrant here required Facebook to disclose information to law enforcement, and the FBI then reviewed that information off-site, consistent with the warrant's protocols.

2. Ninth Circuit and Other Case Law Support the Two-Step Process

In *Flores*, the Ninth Circuit expressly approved this two-step process for electronic evidence from Facebook:

> [Defendant] further argues that the Facebook evidence presented at trial should have been suppressed because the government exceeded its scope by seizing all 11,000 pages of data in [defendant's] account. Pursuant to the terms of the warrant, however, Facebook was authorized to provide agents with a copy of the entire contents of [defendant's] account. Agents then segregated 100 pages of responsive material from the entire account into a separate file within the 90-day period authorized by the warrant. Again pursuant to the warrant, the original copy of [defendant's] account was sealed in an evidence bag and is inaccessible absent a new warrant. In short, the government executed the warrant exactly as it was written.

Flores, 802 F.3d at 1046.

In an opinion from the Southern District of New York, the court analyzed relevant case law and analogized the search of an email account (which is similar to this search warrant for Facebook accounts) to the search of computer hard drives:

> We perceive no constitutionally significant difference between the searches of hard drives . . . and searches of email accounts. Indeed, in many cases, the data in an email account will be less expansive than the information that is typically contained on a hard drive. Therefore, we believe that the case law we have cited concerning searches of hard drives and other storage media supports the Government's ability

> to access an entire email account in order to conduct a search for emails within the limited categories contained in the warrant. *Notably, every case of which we are aware that has entertained a suppression motion relating to the search of an email account has upheld the Government's ability to obtain the entire contents of the email account to determine which particular emails come within the search warrant*. *See United States v. Bach*, 310 F.3d 1063, 1065 (8th Cir.2002) (upholding as constitutionally reasonable the seizure of "all of the information" from defendant's email account where the service provider did not "selectively choose or review the contents of the named account"); *United States v. Ayache*, 2014 WL 923340, at *2-3 (M.D.Tenn. March 10, 2014) (denying motion to suppress "seizure of all emails in a defendant's account [ ] where there was probable cause to believe that the email account contained evidence of a crime"); *United States v. Deppish*, 994 F.Supp.2d 1211, 1219-21 & n. 37 (D.Kan.2014) (noting that "nothing in § 2703 precludes the Government from requesting the full content of a specified email account," and concluding that such a search is not a "general search"); *United States v. Taylor*, 764 F.Supp.2d 230, 232, 237 (D.Me.2011) (upholding search of "all information associated with an identified Microsoft hotmail account"); *United States v. Bowen*, 689 F.Supp.2d 675, 682 (S.D.N.Y. 2010) (Fourth Amendment does not require authorities to "ascertain which e-mails are relevant before copies are obtained from the internet service provider for subsequent searching"); *United States v. McDarrah*, 2006 WL 1997638, at *9-10 (S.D.N.Y. July 17, 2006) (denying motion to suppress seizure of "[a]ll stored electronic mail and other stored content information presently contained in" a specified email account, aff'd, 351 Fed.Appx. 558 (2d Cir.2009).

In re Warrant for All Content and Other Info. Associated with the Email Account xxxxxxx@gmail.com Maintained at Premises Controlled by Google, Inc., 33 F. Supp. 3d 386, 394 (S.D.N.Y. 2014) (emphasis added).

In defendants' Memorandum, defendants unpersuasively rely on opinions from magistrate judges that have been vacated or overruled by district court judges in the same district.[1] For example, *In re Search of Info. Associated with [redacted]@mac.com that is*

[1] Defendants rely heavily on the magistrate opinion of *In re Search of Info. Associated with [redacted]@mac.com that is Stored at Premises Controlled by Apple, Inc*, 25 F. Supp. 3d 1 (D.D.C. 2014). *See* Defs.' Mem. 13-14, 16. However, the Chief Judge for the U.S. District Court for the District of Columbia vacated the magistrate's ruling in a published opinion. *See*

Stored at Premises Controlled by Apple, Inc., 13 F. Supp. 3d 157, 165 (D.D.C. 2014) vacates the opinion cited in the defense's Memorandum and instead holds:

> Several courts have found the two-step procedure to be reasonable under the Fourth Amendment, provided that there is a valid warrant supported by probable cause. *See, e.g.*, *United States v. Schesso*, 730 F.3d 1040, 1046 (9th Cir.2013) (upholding government's seizure of electronic data for a subsequent off-site search where there was a fair probability that evidence would be found on the defendant's personal computer and other electronic devices); *United States v. Evers*, 669 F.3d 645, 652 (6th Cir.2012) ("The federal courts are in agreement that a warrant authorizing the seizure of a defendant's home computer equipment and digital media for a subsequent off-site electronic search is not unreasonable or overbroad, as long as the probable-cause showing in the warrant application and affidavit demonstrate a 'sufficient chance of finding some needles in the computer haystack.'" (quoting *United States v. Upham*, 168 F.3d 532, 535 (1st Cir.1999))).

(Footnote omitted).

The Facebook warrant in this case complied with Rule 41 and satisfied the Fourth Amendment's reasonableness requirement.

C. The Warrant Was Supported by Probable Cause

Defendants argue that the affidavit lacks probable cause to authorize a search of portions of the defendants' Facebook accounts: "In contrast to the narrow category of public postings for which arguably there was probable cause, the search warrant affidavit sought production of

---

13 F. Supp. 3d 157 (D.D.C. 2014) (holding that the "government's application for a search warrant complies with the requirements under the Fourth Amendment and the procedures for executing the warrant are authorized under Rule 41 of the Federal Rules of Criminal Procedure. Accordingly, the magistrate judge's second memorandum opinion and order will be vacated and the government's application for a search warrant will be granted.").

Defendants also cite the magistrate opinion of *In re Applications for Search Warrants for Info. Associated with Target Email Accounts/Skype Accounts*, 2013 WL 4647554 (D. Kan., Jan. 31, 2014). *See* Defs.' Mem. 16. This case was overruled by a district court judge in the District of Kansas in *United States v. Deppish*, 994 F. Supp. 2d 1211, 1221 & n. 45 (D. Kan. 2014).

private Facebook features for which there was no probable cause." Defs.' Mem. 2. In contrast to defendants' claims, the 91-page affidavit in support of the search warrant application thoroughly details defendants' alleged offenses and how defendants used their Facebook accounts as instrumentalities of the charged crimes and in furtherance of the indicted conspiracy.

The affidavit includes dozens of examples of defendants communicating with their codefendants and others using Facebook. The affidavit also outlines how defendants used their Facebook accounts to write comments, post photos and videos, and engage in other social media communications about their occupation of the Malheur National Wildlife Refuge.

For example, the affidavit references numerous instances of the defendants sharing and re-posting each other's Facebook posts. *See, e.g.*, Defs.' Sealed Ex. A to ECF No. 742, ¶¶ 23-26, 28, 30, 34-38, 42, 43, 47, 48, 53, 65, 77, 89, 94. The affidavit also highlights that many of the defendants were Facebook friends with each other. *See, e.g.*, Sealed Ex. A, ¶¶ 25, 31, 35, 39, 48, 76, 84, 85. Paragraph 106 of the affidavit specifically mentions that "Facebook users can exchange private messages on Facebook with other users. These messages, which are similar to email messages, are sent to the recipient's 'Inbox' on Facebook, which also stores copies of messages sent by the recipient as well as other information."

Finally, paragraph 119 of the affidavit further establishes probable cause for the search and seizure of all of the responsive evidence listed in Attachment B to the warrant:

> [I]nformation stored in connection with a Facebook account may provide crucial evidence of the "who, what, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Facebook user's "Neoprint," IP log, stored electronic communications, and other data retained by Facebook, can indicate who has used

> or controlled the Facebook account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, profile contact information, private messaging logs, status updates, and tagged photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Facebook account at a relevant time. Further, Facebook account activity can show how and when the account was accessed or used.

Based on the totality of the affidavit, and the examples provided above, the warrant was supported by a strong demonstration of probable cause to search and seize the responsive items listed in Attachment B.

D. The Agents Acted in Good Faith

As noted above, the Facebook warrant was supported by probable cause. However, a warrant that the defense claims is overbroad and lacking probable cause would still be protected by the "good faith" exception:

> Even if the warrant were deficient, the officers' reliance on it was objectively reasonable and the "good faith" exception to the exclusionary rule applies. *United States v. Leon*, 468 U.S. 897, 104 S.Ct. 3405, 82 L.Ed. 2d 677 (1984) ("[T]he marginal benefit or nonexistent benefits produced by suppressing evidence obtained in objectively reasonable reliance on a subsequently invalidated search warrant cannot justify the substantial costs of exclusion."). The . . . judge was not misled by information in the affidavit, he did not wholly abandon his judicial role, and the affidavit certainly was not "so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable." *Id*. at 923, 104 S.Ct. 3405 (quoting *Brown v. Illinois*, 422 U.S. 590, 611, 95 S.Ct. 2254, 45 L.Ed. 2d 416 (1975) (Powell, J., concurring in part)).

United States v. Schesso, 730 F.3d 1040, 1050 (9th Cir. 2013).

E. Overbreadth Can Be Remedied by Severance

Finally, contrary to defendants' assertions, the remedy for an overly broad warrant would be severance: "We have embraced the doctrine of severance, which allows us to strike from a

warrant those portions that are invalid and preserve those portions that satisfy the Fourth Amendment. Only those articles seized pursuant to the invalid portions need be suppressed." *Flores*, 802 F.3d at 1045 (citation and internal quotation marks omitted). If the Court is inclined to suppress any portion of the Facebook warrant issued by Judge Papak, the government respectfully requests the opportunity to submit supplemental briefing regarding the appropriate scope of severance.

IV. Conclusion

For the reasons set forth above, the government recommends that defendants' Motion to Suppress Evidence from the Oregon Facebook warrant be denied.

Dated this 1st day of July 2016.

Respectfully submitted,

BILLY J. WILLIAMS
United States Attorney

s/ Craig J. Gabriel
ETHAN D. KNIGHT, OSB #992984
GEOFFREY A. BARROW
CRAIG J. GABRIEL, OSB #012571
Assistant United States Attorneys